Functionality	Standards	Implementation Timeline			Certification Criteria
		2011	**2013**	**2015+**	
	Standards Definition [Note 1]	**Implementation Timeline [Note 2]**			
Access Control	45 CFR Parts 160, 162, and 164 Health Insurance Reform: Security Standards; Final Rule. February 20, 2003. § 164.312(a) Access Control (HIPAA)	HIPAA + AES	HIPAA + AES + HL7 RBAC + SAML + WS-Trust	HIPAA + AES + HL7 RBAC + XACML + SAML + WS-Trust	• Provide capability to allow access only to those persons or software programs that have been granted access rights. • Provide capability to assign a unique name and/or number for identifying and tracking user identity. • Provide capability to access necessary electronic protected health information during an emergency. • Provide capability to terminate an electronic session after a predetermined time of inactivity. • Provide the capability to encrypt and decrypt electronic protected health information.
	FIPS 197, Advanced Encryption Standard, Nov 2001				Provide the capability to encrypt data at rest using AES.
	HL7 V3 RBAC, R1-2008, HL7 Version 3 Standard: Role Based Access Control (RBAC) Healthcare Permissions Catalog, Release 1, February 2008				Provide the capability to represent role-based permissions as {operation,object} pairs, using the HL7 permission vocabulary.
	OASIS eXtensible Access Control Markup Language (XACML), ITU-T Recommendation X.1142, February 2005				Provide the capability to use XACML access-control policy language and processing model to record and exchange access control information between security domains.
	OASIS Security Assertion Markup Language (SAML) v2.0 OASIS Standard, ITU-T X.1141				Provide the capability exchange user authentication and authorization informaiton between security domains, using the SAML framework.
	OASIS WS-Trust Version 1.3, March 2007				Provide the capability to request and issue security tokens, and to broker trust relationships using WS-Trust.

October 2009 - Certification Standards Recommendations: PRODUCT CERTIFICATION STANDARDS

Functionality	Standards	Implementation Timeline			Certification Criteria
		2011	2013	2015+	
	Standards Definition [Note 1]	**Implementation Timeline [Note 2]**			
Audit	45 CFR Parts 160, 162, and 164 Health Insurance Reform: Security Standards; Final Rule. February 20, 2003. § 164.312(b) Audit Controls (HIPAA)	HIPAA + ATNA	HIPAA + ATNA	HIPAA + ATNA	Provide the capability to record and examine activity in information systems that contain or use electronic protected health information.
	IHE ITI-TF Revision 4.0 or later, Audit Trail and Node Authentication (ATNA) Integration Profile, Section 9.1 Authentication				Provide the capability to use the ATNA profile to communicate audit messages between Secure Nodes and to establish Audit Repository nodes to collect audit information.

Functionality	Standards	Implementation Timeline			Certification Criteria
		2011	**2013**	**2015+**	
	Standards Definition [Note 1]	**Implementation Timeline [Note 2]**			
Authentication	45 CFR Parts 160, 162, and 164 Health Insurance Reform: Security Standards; Final Rule. February 20, 2003. § 164.312(d) Person or Entity Authentication (HIPAA)	HIPAA(a)	HIPAA(a) + HIPAA(b) + XUA	HIPAA(a) + HIPAA(b) + XUA	(a) Person or entity authentication: Provide the capability to verify that a person or entity seeking access to electronic protected health information is the one claimed.
					(b) • Provide an authentication mechanism that requires the claimant to prove through a secure authentication protocol that he or she controls the token (e.g., password, private key) presented, and that protects against online guessing, replay, session hijacking, and eavesdropping attacks. • If the authentication mechanism is designed to use long-term shared authentication secrets, implement such that the system never reveals these secrets to any party except the claimant and verifiers that are operated by the credential service provider. • If the system communicates authentication results to third parties (i.e., shares assertions), implement the capability such that all assertions and assertion references are protected from fabrication, modification and reuse attacks, and resistant to disclosure, redirection, capture, and substitution attacks.
	IHE ITI-TF Volume 2 Supplement 2007 – 2008 Cross Enterprise User Assertion (XUA)				Provide the capability to communicate claims about an identity of an authenticated principal (e.g., user, application, system) in transactions that cross enterprise boundaries, as defined in the XUA profile.

Functionality	Standards	Implementation Timeline			Certification Criteria
		2011	**2013**	**2015+**	
	Standards Definition [Note 1]	**Implementation Timeline [Note 2]**			
Consent Management	45 CFR Parts 160 and 164. Standards for Privacy of Individually Identifiable Health Information; Final Rule. August 14, 2002; American Recovery and Reinvestment Act of 2009 (ARRA), Subtitle D - Privacy. January 6, 2009 (HIPAA)	HIPAA	HIPAA + (CAP143 or BPPC)	HIPAA + (CAP143 or BPPC) + HL7 PrivacyCodes	Provide the capability to electronically record individual consumers' consents and authorizations.
	HITSP/CAP143 Manage Consumer Preference and Consents				Provide the capability to capture and manage consumer consents and authorizations as CDA documents, as described in CAP143.
	IHE ITI-TF Revision 5.0, Basic Patient Privacy Consents (BPPC) Profile				Provide the capability to record consumers' privacy consents and authorizations; to tag documents published to XDS with the privacy consent that was used to authorize the publication; and to enforce the privacy consent appropriate to each use.
	HL7 Version 3.0 Privacy Consent related specifications RCMR_RM010001 - Data Consent				Provide the capability to record consumer consents and authorizations using HL7 V3 privacy consent codes.

Functionality	Standards	Implementation Timeline			Certification Criteria
		2011	2013	2015+	
	Standards Definition [Note 1]	**Implementation Timeline [Note 2]**			
Consumer EHR	45 CFR Parts 160 and 164. Standards for Privacy of Individually Identifiable Health Information; Final Rule. August 14, 2002; American Recovery and Reinvestment Act of 2009 (ARRA), Subtitle D - Privacy. January 6, 2009 (HIPAA)	HIPAA + CAP120	HIPAA + CAP119	HIPAA + CAP119	Provide the capability to create an electronic copy of an individual's electronic health record, to record it on removable media, and to transmit it to a designated entity capable of receiving electronic transmissions.
	HITSP/CAP120 Communicate Unstructured Document (using portable media or system-to-system (PHR) topology)				Provide the capability to create and distribute an electronic copy of an individual's EHR as an unstructured document.
	HITSP/CAP119 Communicate Structured Document (using portable media or system-to-system (PHR) topology)				Provide the capability to create and distribute an electronic copy of an individual's EHR as a structured Continuity of Care Document (CCD).

Functionality	Standards	Implementation Timeline			Certification Criteria
		2011	**2013**	**2015+**	
	Standards Definition [Note 1]	**Implementation Timeline [Note 2]**			
HIPAA Deidentification	45 CFR Parts 160 and 164. Standards for Privacy of Individually Identifiable Health Information; Final Rule. August 14, 2002. Section 164.514(a-b) Deidentification of protected health information (HIPAA)	HIPAA De-identification + HIPAA Re-identification + ISO Pseudony-mization	HIPAA De-identification + HIPAA Re-identification + ISO Pseudony-mization + HL7 V3 Pedigree	HIPAA De-identification + HIPAA Re-identification + HL7 V3 Pedigree + ISO Pseudo-nymization	Provide the capability to remove the identifiers enumerated in Section 164.514(b)(2)(i) of the HIPAA Privacy Rule.
	46 CFR Parts 160 and 164. Standards for Privacy of Individually Identifiable Health Information; Final Rule. August 14, 2002. Section 164.514(c) Reidentification (HIPAA)				• Provide the capability to generate and assign a code or other means of record identification to allow information de-identified in accordance with the HIPAA Privacy Rule to be re-identified by the covered entity; such code or other means must not be derived from or related to the information and must not be otherwise capable of being translated so as to disclose the identity of the individual. • Provide the capability to protect the code or other means of record identification from unauthorized disclosure.
	HL7 Version 3.0 Clinical Genomics; Pedigree, Release 1 (Anonymization)				If the system is capable of persisting and exchanging genomic data, provide the capability to anonymize genomic data using the Pedigree approach.
	ISO/TS 25237:2008 Health Informatics -- Pseudonymisation, Unpublished Technical Specification (Pseudonymization)				Use ISO/TS 25237 as guidance in the implementation of pseudonymization capabilities.

Functionality	Standards	Implementation Timeline			Certification Criteria
		2011	2013	2015+	
	Standards Definition [Note 1]	**Implementation Timeline [Note 2]**			
Data Integrity	45 CFR Parts 160, 162, and 164 Health Insurance Reform: Security Standards; Final Rule. February 20, 2003. § 164.312(c) Integrity (HIPAA)	HIPAA + SHA + ASTM-Auth	HIPAA + SHA + ASTM-Auth	HIPAA + SHA + ASTM-Auth + (DSG + XadES + TS-17090)	• Provide the capability to protect electronic protected health information from improper alteration or destruction. • Provide electronic mechanisms to corroborate that electronic protected health information has not been altered or destroyed in an unauthorized manner.
	FIPS PUB 180-2 with change notice to include SHA-224. 1 August 2002. SHA-2 family (excludes SHA-1)				Provide the capability to use SHA to protect the integrity of data at rest.
	ASTM Standard Guide for Electronic Authentication of Health Care Information: # E1762-95(2003)				Use as guidance in the design and implementation of electronic signatures.
	HIE ITI-TF Supplement Volume 3 – Document Digital Signature (DSG) Content Profile				Provide the capability to digitally sign documents shared between organizations, using XAdES advanced electronic signatures. Use ISO/TS-17090 as guidance in implementing the use of digital certificates to digitally sign electronic documents using DSG.
	ETSI Technical Specification TS 101 903: XML Advanced Electronic Signatures (XadES)				
	ISO/TS-17090, Health Informatics, Public Key Infrastructure				

Functionality	Standards	Implementation Timeline			Certification Criteria
		2011	**2013**	**2015+**	
	Standards Definition [Note 1]	**Implementation Timeline [Note 2]**			
Transmission Security	45 CFR Parts 160, 162, and 164 Health Insurance Reform: Security Standards; Final Rule. February 20, 2003. § 164.312(d) Transmission Security (HIPAA)	HIPAA + SHA-2 + AES + TLS	HIPAA + SHA-2 + AES + TLS	HIPAA + SHA-2 + AES + TLS + CMS	• Implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network. • Integrity controls. Implement security measures to ensure that electronically transmitted electronic protected health information is not improperly modified without detection until disposed of. • Encryption. Implement a mechanism to encrypt electronic protected health information whenever deemed appropriate.
	FIPS PUB 180-2 with change notice to include SHA-224. 1 August 2002. SHA-2 family (excludes SHA-1)				Provide the capability to use SHA to protect the integrity of data transmissions.
	FIPS 197, Advanced Encryption Standard, Nov 2001				Provide the capability to use AES to encrypt data for transmission.
	IETF Transport Layer Security (TLS) Protocol: RFC 2246, RFC 3546				Provide the capability to use TLS (with SHA-2 and AES) to establish a mutually authenticated, encrypted, and integrity-protected channel for data exchanges over the World Wide Web.
	IETF Cryptographic Message Syntax (CMS), RFC-2630, -3852				If an email capability is provided, implement the CMS standard to cryptographically protect messages, including digital signatures, message digest, message authentication, and content encryption.

Functionality	Standards	Implementation Timeline			Certification Criteria
		2011	**2013**	**2015+**	
	Standards Definition [Note 1]	**Implementation Timeline [Note 2]**			
Consistent Time	IETF Network Time Protocol (Version 3) Specification, Implementation and Analysis, "Request for Comment" (RFC) #1305, March, 1992	CT + (NTP or SNTP)	CT + (NTP or SNTP)	CT + (NTP or SNTP)	Provide the capability to use NTP to enable a Time Server to provide time to a Time Client.
	IETF Simple Network Time Protocol (SNTP) Version 4, "Request for Comment" (RFC) #2030, October, 1996				Provide the capability for Time Clients that are not grouped with a Time Server to use SNTP to obtain time.
	IHE ITI-TF Revision 4.0 or later, Consistent Time (CT) Integration Profile				Provide the capability to synchronize the time base between multiple actors and computers using the mechanisms described in the IHE CT profile.

October 2009 - Certification Standards Recommendations: INFRASTRUCTURE CERTIFICATION STANDARDS

Functionality	Standards	Implementation Timeline			Certification Criteria
		2011	**2013**	**2015+**	
	Standards Definition [Note 1]	**Implementation Timeline [Note 2]**			
Document Exchange	HITSP/SC112 - Healthcare Document Management	SC112	SC112 + HL7 Confidentiality Codes + {(XDS.b + RegQuery + ebXML RIM + ebRS) or XDR or XCA or XDM}	SC112 + HL7 Confidentiality Codes + {(XDS.b + RegQuery + ebXML RIM + ebRS) or XDR or XCA or XDM}	Provide the capability to share healthcare documents using a set of topologies, such as Media, e-Mail, Point-to-Point, Shared within a Health Information Exchange, and Shared within a larger community (made up of potentially diverse Health Information Exchanges).
	IHE ITI-TF Cross Enterprise Document Reliable Interchange (XDR) Integration Profile				Provide the capability to reliably and automatically transfer electronic documents and metadata for one patient between EHR systems in the absence of an XDS infrastructure, in accordance with the XDR integration profile.
	IHE ITI-TF Revision 5.0 Volume 2 Supplement 2007 – 2008 Cross-Enterprise Document Sharing-B (XDS.b) Integration Profile				Provide the capability to share electronic documents between healthcare enterprises through federated document repositories and a document registry, as defined in the XDS.b integration profile, including Registry Stored Query Transaction profile, OASIS ebXML Registry Information Model, and OASIS ebXML Registry Services specifications.
	IHE ITI-TF Revision 5.0 - Registry Stored Query Transaction for XDS Profile Supplement [ITI-18]				
	OASIS/ebXML Registry Information Model v3.0				
	OASIS/ebXML Registry Services (ebRS) Specifications v3.0				
	IHE ITI-TF Revision 5.0 or later, Cross Community Access (XCA) profile				Provide the capability to query and retrieve patient-specific medical data held by other communities (e.g., facilities, enterprises) that have agreed to work together using a common set of policies for the purpose of sharing clinical information via an established mechanism. Such communities may be XDS Affinity Domains or any other communities, no matter what their internal sharing structure.
	IHE ITI-TF Revision 5.0 or later, Cross-Enterprise Document Media Interchange (XDM) Integration Profile				Provide the capability to exchange an electronic document stored on removable media (e.g., CD, USB drive) or as a ZIP file attached to secured email.
	HL7 V3 Confidentiality Codes value set				Provide the capability to indicate document sensitivity using metadata containing HL7 confidentiality codes.

Functionality	Standards	Implementation Timeline			Certification Criteria
		2011	**2013**	**2015+**	
	Standards Definition [Note 1]	**Implementation Timeline [Note 2]**			
Service Access	OASIS Simple Object Access Protocol (SOAP) Version 1.2	(SOAP + WS-Security) or REST	(SOAP + WS-Security) or REST	(SOAP + WS-Security) or REST	For implementations of integration profiles that allow for the use of either SOAP or REST, either SOAP or REST may be used, consistent with the implementation guidance provided by the relevant integration profile.
	OASIS Web Services Security:SOAP Message Security 1.1 (WS-Security 2004), 1 February 2006				If SOAP is used to access web services, implement WS-Security security services.
Domain Name Service	IETF: RFC-2181, -2219, -2782. Domain Name Service (DNS) services	DNS	DNS	DNS	Provide the capability to resolve Internet domain names using DNS.
Directory Access	IETF: RFC-2251, -2252, -2253. Lightweight Directory Access Protocol (LDAP)	LDAP	LDAP + (PWP + RFC1766)	LDAP + (PWP + RFC1766)	Provide the capability to perform intra-enterprise and cross-enterprise directory look-up functions using LDAP.
	IHE ITI-TF Revision 4.0 or later, Personnel White Pages (PWP)				Provide the capability to perform intra-enterprise and cross-enterprise directory look-up functions using PWP.
	RFC 1766 Tags for the Identification of Languages				Use RFC 1766 language tags to indicate language preferences in PWP.

NOTES:

1. Standards Definition: Includes regulatory standards, standards developed by Standards Development Organizations (SDOs), and standards developed by Profile-Enforcement Organizations (PEOs)

2. Implementation Timeline Note: Minimal standards for targeted year. Earlier implementation of standards specified for 2013 or 2015 is encouraged.